Slide 1

Good day Mr. Chairman, members of the Board. For the record, I am Dr. Charles Martin, a Senior Technical Specialist on the staff of the Defense Nuclear Facilities Safety Board. While I principally review the safety bases for nuclear explosive operations at the Pantex Plant and for Stockpile Stewardship activities at Los Alamos National Laboratory, I have also been leading staff efforts to improve quality assurance of safety-related software used by the Department of Energy. In addition, I was a principal author of DNFSB/TECH-25, *Quality Assurance for Safety-Related Software at the Department of Energy Defense Nuclear Facilities.*

Today I will provide some observations by the Board's staff regarding software quality assurance at the Department of Energy.

Slide 2

Software is used for many safety-related activities at the Department. These include, for example, the analysis of hazards to determine the safety significance of structures, systems, components. Software is also used in the detailed design process to ensure that structures, systems, and components which have been designated as safety-related are sufficiently robust to reliably perform their safety functions during credible accident conditions. In addition, software is used to perform automatic control functions for such safety systems. And finally, software is used to provide supporting functions to the overall safety program. One example is the linking database at the Pantex Plant which is used as a tool for the change control process. This database provides a linkage between safety basis documents and the controls which are relied upon for safety, so that if a change is made to the safety basis, the software identifies the controls which are affected by the change.

Clearly, the safety posture of many Department of Energy nuclear facilities depends on the correct operation of the software used for their design, analysis, and operation.

Slide 3

During 1999, the Board’s staff had noted numerous problems with software at the Department of Energy. Several codes used for safety analysis were reported to have deficiencies. Subsequent follow-up revealed that those codes did not have adequate verification and validation testing performed during development. In addition control software at the Los Alamos Critical Experiments Facility had caused an uncontrolled reactivity insertion. And a search of the Occurrence Reporting and Processing System yielded more than 150 reportable occurrences involving programmable logic devices. These issues and others were communicated to the Department in DNFSB/TECH-25 in January, 2000. In the transmittal letter to the Deputy Secretary, the Board asked the Department for a plan of action to address the software quality concerns raised in the report.

The Board received the Department’s corrective action plan on October 3, 2000, over six months past the due date. Unfortunately, the report was not sufficiently responsive to the Board’s concerns.

Slide 4

On October 23, the Board asked the Department to correct the following deficiencies in the corrective action plan: Some actions in the plan were to be performed before the true nature of the problems were understood. In addition, the plan was based on a survey, rather than on-site assessments, raising concerns for the accuracy and completeness of the information upon which the plan was based. Beyond this, the proposed approach has the effect of separating software quality assurance from the overall quality assurance process under 10 CFR 830 and DOE Order 414.1A. And, since the Safety Analysis Software Group was not formed until 2001, key subject matter experts were not adequately involved in developing the plan. The Board was also concerned about the leadership and funding provisions in the plan.

While several deliverables under the existing flawed plan have been received and have provided some useful information, it appeared that the approach used was unlikely to reveal the true depth and breadth of the issues or to suggest the best solutions. At this point, the Board has still not been provided with an acceptable plan.

Slide 5

The Board decided to independently pursue a course of investigation into the software quality assurance practices by other industries and to perform detailed on-site reviews of software practices at several Department of Energy sites. These actions were taken in order to better understand the issues.

The Board held two public meetings in which software quality assurance was a special interest item; this is the third such public meeting. In addition, the Board's staff visited the NASA independent verification and validation facility in West Virginia, and has visited four Department of Energy sites with defense nuclear facilities to assess their programs in detail. These sites included the Y-12 National Security Complex at Oak Ridge, Tennessee; Sandia National Laboratories, in Albuquerque, New Mexico; the Hanford Reservation in Washington state; and the Pantex Plant near Amarillo, Texas.

Slide 6

The following charts summarize the key observations made by the staff as a result of these activities.

First, while there is some good guidance in the DOE directives on software quality assurance, the method used to promulgate these requirements does not clearly set expectations for software quality assurance, particularly for safety-related software. If you will forgive the metaphor, this approach is akin to "throwing the hay out where the goats can get it." As a result, contractors have developed their own programs. On-site reviews have shown that contractor implementing procedures do not have sufficient detail to define a robust process or ensure high quality software products are produced.

Responsibilities and authorities for the safety-related aspects of software quality are not clearly defined, nor is there an effective champion for software quality assurance within the Department. This is a complicated problem since the Clinger-Cohen Act assigns certain policy and oversight responsibilities to the Chief Information Officer, but safety policy and oversight responsibilities lie elsewhere. And the problem is further complicated by the recent reorganization in the Department. As a result, there is a lack of DOE oversight.

Slide 7

It is perhaps no surprise that there is no consensus set of training requirements for software quality assurance, because, as we have just seen, there is no clearly defined set of software quality assurance requirements. As a result, there is no formal DOE training program for software quality assurance, and most contractors do not have formal software quality assurance training programs. This was also a finding in the Department's Training Focus Area Team report, *Summary Report on Training to Department of Energy Lead Principal Secretarial Officers.*

Slide 8

During discussions with individuals from NASA, the Department of Defense, the chemical industry, and the nuclear industry, it was clear to all that software errors can be hard to find, particularly for complex programs. As a result, there is a need for both a rigorous, well documented process to develop safety-related software, and that certain key actions must be taken to ensure the products will perform correctly and safely. The staff believes adequate consensus standards exist for most software quality assurance process steps, for example IEEE 830, *Software Requirements Specifications,* and IEEE 1008, *Software Unit Testing*.

But, because software technology continues to evolve, the guidance for how to engineer safety-related software also needs to evolve. Interagency working groups are attempting to fill the existing gaps, and such groups will also address future evolutions with respect to software safety. The Department should consider becoming a partner with other agencies in such endeavors.

No Slide

Finally, I would like to offer for the record, that several relevant papers were presented at the 11th Annual DOE Facility Safety Analysis Working Group Workshop during a session which I chaired entitled *Assessing Computational Tools and Software Upgrades*. This meeting was held in Milwaukee, Wisconsin as an embedded topical during the American Nuclear Society's Annual Meeting in June 2001. The proceedings are available from the American Nuclear Society at www.ans.org.

Thank you Mr. Chairman.